North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

4 cars derail from RRVW train in Leonard, N.D. Authorities are investigating the derailment of four cars on a Red River Valley & Western train in Leonard, North Dakota. A Cass County sheriff's deputy said no hazardous materials were in the rail cars that derailed about 10 p.m. November 2. No injuries were reported. The cause of the derailment is under investigation. Source: http://www.grandforksherald.com/event/article/id/182016/group/homepage/

Regional

(Michigan) **Early detection program finds a new invasive pest of fruit in Michigan.** Spotted Wing Drosophila (Drosophila suzukii), or SWD, a small vinegar fly native to Asia, has been found in traps deployed this year by Michigan State University (MSU) entomologists in southwestern Michigan. This pest is established in the western United States, damaging fruit in California and the Pacific Northwest, but this is the first time it has been found in the Midwest. SWD is a pest of berry crops, cherries, grapes, and tree fruit. No flies were trapped in Michigan through the summer months in 2010, but in late September and early October, monitoring traps in southwestern Michigan picked up male and female SWD. This pest has not been found in any fruit, and flies were trapped only after crop harvest was complete. Source: http://www.hillsdale.net/news/camden/x1272817509/Early-detection-program-finds-a-new-invasive-pest-of-fruit-in-Michigan

(Michigan) **Wolf attacks on U.P. farms a growing concern.** Michigan's gray wolves have attacked Upper Peninsula farms more times in 2010 than in the past 3 years combined, killing a record number of livestock as state officials continue to push to remove federal protections for the endangered animal. Farmers are reimbursed by the state for livestock killed in confirmed attacks, but the process can be frustrating because federal law leaves landowners and wildlife officials hamstrung in dealing with repeated attacks from rogue wolf packs, officials said. Two dogs, 57 cattle, seven sheep, and a guinea hen have fallen victim to wolves this year. Sixteen animals were killed in 2009. Michigan officials said it is a small percentage of Michigan's 557 gray wolves that prey on domestic animals from farms across the Upper Peninsula. Wolves are protected under the Endangered Species Act and are illegal to kill except in defense of human life. Source: http://www.mlive.com/outdoors/index.ssf/2010/10/wolf_attacks_on_up_farms_a_gro.html

(Montana) **Bozeman outage darkens 4,500 homes.** A power outage affected about 4,500 NorthWestern Energy customers on Bozeman, Montana's west side November 2, a company spokeswoman said. The power went out at about 8:45 p.m. A faulty relay at an electrical substation caused the outage. The spokeswoman did not know the geographical extent of the outage, but said power was expected to be completely restored by midnight. The outage affected neighborhoods from Huffine Lane almost to Interstate 90 between Four Corners and North 19th Avenue, a Bozeman police sergeant said. A dispatcher at the county's 911 call center off Davis Road said at 10 p.m. the center was operating on backup electrical service. Partial power was restored to the North 19th

Avenue area just before 10:30 p.m. Although police were busy patrolling and directing traffic where signals were down, there were no "specifically related outage problems," the sergeant said. Source: http://www.bozemandailychronicle.com/news/article_df1c21ae-e716-11df-b45d-001cc4c002e0.html

(Montana) **Brucellosis found in bison on Ted Turner ranch.** A bacterial disease has been found in a 4,600-head bison herd in Montana, the first time brucellosis has been discovered in a domestic herd in the state in more than 2 years. The disease, which can cause pregnant bison, cattle, and elk to abort their fetuses, was found in a 7-year-old cow about 2 weeks ago and is suspected in two other bison on the ranch, a state veterinarian said. The cow has been killed and the other two have been quarantined from the rest of the herd pending test results, he said. They also will be slaughtered after the testing is completed. Officials have testedmost of the 2,000 animals on the ranch that livestock officials have determined could carry the disease. An investigation is under way to trace the source of the infection anto find out whether it has spread. Source: http://www.necn.com/11/01/10/Brucellosis-found-in-bison-on-Ted-Turner/landing_scitech.html?&blockID=3&apID=68b67926906446ce8996cd8986858f2

National

New Yorker accused of plan to attack US troops. A New York man accused of trying to join the U.S. military with the intent of attacking U.S. troops in Iraq did not enter a plea as he faced a U.S. judge November 2 in New York. The 21-year-old U.S. citizen was arrested October 22 in Hawaii and transferred to the U.S. District court in Brooklyn, where he is charged with making materially false statements in a matter involving international terrorism. He faces 8 years in prison. Source: http://af.reuters.com/article/somaliaNews/idAFN0224303220101102

MSHA urges miners and mine operators at underground coal mines to follow safety checklists. The Mine Safety and Health Administration (MHSA) kicked off its 2010 Winter Alert campaign to warn miners and mine operators about the dangers colder weather can bring to the mining environment. Historically, statistics show most coal mine explosions occur during the colder months. Low barometric pressures and low humidity, coupled with seasonal drying of many areas in underground coal mines, have contributed to the larger number of mine explosions during winter months. Other hazards include limited visibility, icy haulage roads and walkways, and the freezing and thawing effect on highwalls at surface mines. MSHA urges miners and mine operators at underground coal mines to follow safety checklists by ensuring there is adequate ventilation, applying liberal amounts of rock dust, conducting frequent and thorough examinations, and being familiar with emergency procedures to prevent coal mine ignitions and explosions. Miners also should be vigilant about keeping escapeways clear of impediments. Miners and operators of surface mines should examine the stability of highwalls, remove snow and ice from walkways, de-ice any equipment, and apply salt and sand liberally where needed. During their normal inspection duties, MSHA inspectors will distribute posters and hardhat stickers with the slogan "Beat Winter Hazards, Win with Winter Alert" to alert miners about potential risks. Source: http://coalgeology.com/msha-urges-miners-and-mine-operators-at-underground-coal-mines-to-follow-safety-checklists/8233/

(California) **Man convicted of scheming to import missiles from China.** A jury has convicted a California man of conspiring to import surface-to-air missiles into the United States from China. The man was found guilty of conspiring to smuggle Chinese-made QW-2 shoulder-fired missiles and

counterfeit cigarettes into the country. The man is the first person to be convicted by a jury under 18 U.S.C. Â§ 2332g, an anti-terrorism law prohibiting the importation of missiles that can be used to destroy aircraft. He faces a mandatory minimum prison term of 25 years when he is sentenced in February 2011, prosecutors said. In September 2005, the man and a co-conspirator negotiated with an undercover FBI agent to have several QW-2 missiles and associated hardware transported to the United States from China. Agents arrested both men before the missiles could be shipped. Source: http://westlawnews.thomson.com/California_Litigation/Insight/2010/11_-_November/Man_convicted_of_scheming_to_import_missiles_from_China/

With eyes on Gulf, BP Alaska pipes remain at risk. The extensive pipeline system that moves oil, gas, and waste throughout BP's operations in Alaska is plagued by severe corrosion, according to an internal maintenance report generated 4 weeks ago. The document shows that as of October 1, at least 148 pipelines on Alaska's North Slope received an "F-rank'' from BP. According to BP oil workers, that means inspections have determined more than 80 percent of the pipe wall is corroded and could rupture. Most of those lines carry toxic or flammable substances. Many of the metal walls of the F-ranked pipes are worn to within a few thousandths of an inch of bursting, according to the document, risking an explosion or spills. BP oil workers also said fire and gas warning systems are unreliable, giant turbines that pump oil and gas are aging, and some oil and waste holding tanks are verging on collapse. A BP Alaska spokesman said the company has "an aggressive and comprehensive pipeline inspection and maintenance program," which includes spending millions of dollars and regularly testing for safety, reliability and corrosion. He said that while an F-rank is serious, it does not necessarily mean there is a current safety risk. He added BP would immediately reduce the operating pressure in worrisome lines until it completes repairs. The spokesman noted BP has more than 1,600 miles of pipelines, and does more than 100,000 inspections per year. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/02/AR2010110207033.html

INTERNATIONAL

Explosive packages sent to leaders of Germany, Italy. The discovery of a number of packages originating in Greece containing bombs, including ones addressed to leaders of Germany and Italy, led Greece's Public Order Ministry to announce November 3 that it was suspending for 48 hours all air shipments of packages to other countries. A package containing explosives was found at the office of Germany's chancellor November 2 and was handed over to police. The package had been shipped via cargo plane from Greece. Greece saw a wave of attempted bombings November 1 and 2. Police destroyed the package sent to the German chancellor in a controlled explosion; no one was hurt. The package was found during a routine inspection in the office mailroom. In addition, two other parcels containing explosives were discovered in the cargo section of the Athens airport, a police spokesman said. They were addressed to the European Union law enforcement agency (Europol), based in The Hague, Netherlands, and the European Court of Justice in Luxembourg. In Bologna, Italy, police said they found a package containing an explosive device addressed to the prime minister. Authorities offered no details of what type of explosive the package contained except to say that while detonating it, it produced a "burst of flame," a police officer said. Source: http://edition.cnn.com/2010/WORLD/europe/11/02/germany.suspicious.package/?hpt=T2

Hungary threatened by new chemical disaster, experts warn. Environmentalists have warned of a new industrial accident in Hungary that they said could once again threaten villages, towns and even Budapest with toxic red sludge. Just outside the Hungarian capital, a reservoir is being watched that has potentially similar problems as the one that collapsed in western Hungary in early October, killing at least nine people and injuring over 120 others. The factory in Almasfuzito, once the pride of communist Eastern Europe, was forced to close in the 1990s amid market reforms. More than 1,000 people lost their jobs. The plant left behind a gigantic decrepit reservoir complex filled with toxic red sludge,a byproduct of the conversion of bauxite for use in aluminum production. Seven pools hold 12 million tons of the hazardous waste produced since 1945, more than than 10 times the amount of Hungary's deadly October 4 toxic spill. In that accident the collapse of a reservoir of a metals plant near the western village of Kolontar, caused a catastrophe. There are now concerns a similar accident will occur in Almasfuzito. Even the facility's manager admitted there are dangers. He said earthquakes could happen in the area where the former plant is located. Another problem is frequent flooding from the Danube River, but he said his workers constantly monitor the reservoir. Source: http://www.voanews.com/english/news/Hungary-Threatened-By-New-Chemical-Disaster-Experts-Warn-106437578.html

Greek mail bombers target 5 embassies. Small mail bombs exploded outside the Russian and Swiss embassies in Athens, Greece, November 2, and police destroyed at least three more as they tried to halt a wave of attacks on foreign missions blamed on far-left domestic extremists. Authorities closed down sections of the capital and checked dozens of potential targets, while all embassies were given additional police security. No group claimed responsibility for the attacks, which caused no injuries. No warning was given. No link has been made with the recently discovered Yemen-based mail bomb plot, which used much more powerful devices. The attacks began November 1, when a mail bomb addressed to the Mexican embassy exploded at a delivery service in central Athens, lightly wounding one worker. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/02/AR2010110201349.html?hpid=moreheadlines

British Nuclear Power Plant goes dark. Stuxnet worm to blame. British Energy, owned by France's EDF Energy PLC, has reported an "unplanned outage" at its Heysham 1 nuclear power plant October 31. A company spokesperson told the Associated Press repairs to one of the reactors are ongoing, but did not say when the plant was expected to resume operations. According to Siemens' Web site, EDF Energy is a customer of the German technology giant, whose infrastructure software has suffered from a global infection of the sophisticated Stuxnet worm. A 2007 briefing deck by the Technical Working Group on Nuclear Power Plant Control and Instrumentation disclosed that Heysham 2 had its Reypac controllers replaced with Siemens S7. One expert was not sure if Heysham 1 had the same upgrades as Heysham 2. Source: http://blogs.forbes.com/firewall/2010/11/01/british-nuclear-power-plant-goes-dark-stuxnet-worm-to-blame/

Second reactor eyed at Ginna. A French company has acquired land in New York near the Robert E. Ginna nuclear power plant in Wayne County and the Nine Mile Point plant in Oswego County for possible new reactors. Electricite de France SA said it has purchased Constellation Energy Group's interest in a mutual subsidiary, UniStar Nuclear Energy, for $140 million. Unistar owns the land that could be used for new reactors. So far, EDF — a major European and U.S. energy player with 169,000 employees worldwide — has applied to the Nuclear Regulatory Commission for only one such license, for a new reactor at the Calvert Cliffs nuclear plant in Calvert County, Maryland. "There's nothing on

the drawing board," said the supervisor of Ontario where the Ginna plant is located. He said he supports another reactor and regularly meets with Constellation Energy officials. An EDF spokesman in New York City confirmed the French company has long-term plans for both the Ginna site and the Nine Mile Point site on Lake Ontario north of Syracuse. Source: http://www.democratandchronicle.com/article/20101102/BUSINESS/11020319/1001/Second-reactor-eyed-at-Ginna

Al Qaeda suspected in Yemen oil pipeline blast. Suspected al Qaeda militants blew up a small oil pipeline in southern Yemen November 2, local officials said, the same day the country launched a hunt for those responsible for a plot to mail bombs to the United States. The pipeline in the province of Shabwa was operated by a South Korean firm, officials said, but declined to give further details. It was not clear if exports would be affected. The blast on the pipeline taking crude oil to a maritime export terminal was caused by a timed device, a local security official told Reuters, adding that members of al Qaeda were believed to be behind the attack. Security forces were sent to the province of Maarib and also to Shabwa. Al Qaeda has in the past threatened to target Yemen's oil and gas infrastructure, but such attacks have been relatively rare. Disgruntled tribes have sporadically blown up pipelines to pressure the government. Last month, a gunman believed to have links to al Qaeda killed a Frenchman at Austrian oil and gas company OMV's site in Sanaa. The Yemen wing of the global militant network, Al Qaeda in the Arabian Peninsula, has strongholds in Maarib and Shabwa, where oil and gas fields of international companies are located. Source: http://www.reuters.com/article/idUSLDE6A11NI20101102

Widespread flooding forces evacuation of 3,000. Floods brought by overnight rain have caused the evacuation of more than 3,000 people in Perlis, Kedah, and Terengganu in Malaysia, October 31, and are threatening to force people out of their homes in Kelantan as well. There are fears the situation may worsen because the meteorological services department has warned of heavy rain through Novermber 3. In Perlis, 1,096 people had been moved to nine relief centers, and the six sluice gates of the Timah Tasoh Dam have been opened as the water level at the dam was high. Source: http://www.nst.com.my/nst/articles/Widespreadfloodingforcesevacuationof3_000/Article/

Banking and Finance Industry

Phishing scam targets military families. A new phishing scam is taking aim at members of the U.S. military and their families, using unsolicited e-mails purportedly from United States Automobile Association (USAA), one of the nation's largest financial services and insurance companies, to trick people into divulging their personal information to identity thieves. USAA and the Navy Federal Credit Union in May were hit by a similar phishing scam that also attempted to extract Social Security numbers, credit card numbers, birth dates and other information used to either pilfer bank accounts or steal unsuspecting users' identities. This time around, according to an advisory on security software maker AppRiver's Web site, the con artists are sending a slew of unsolicited e-mails with subject titles, such as "USAA Notification" or "Urgent Message for USAA customer" in the hope of getting just a small fraction of a percentage of recipients to click on a link embedded in the missive. According to the Anti-Phishing Working Group, a consortium of Web retailing, software, security and financial firms, more than 126,000 fake Web sites designed solely to steal users' personal information were discovered in the first half of this year alone. Source:

http://www.esecurityplanet.com/features/article.php/3911141/Phishing-Scam-Targets-Military-Families.htm

(New York) **Civic Center credit card breach may ba computer hack.** Investigators believe scammers used either a skimming device or a computer hack to steal credit and debit card information from victims that had used their cards at the Onondaga County Civic Center in Syracuse, New York. Police have now heard from more than 60 victims. So far, Syracuse Police said most of the victims have reported using their credit or debit card in the basement at the cafeteria of the civic center. One of those victims said his bank called him a few days ago to check on some irregular charges made at the Long Island Rail Road. "The bank had paid five to six transactions, almost $800," he said. While police are not sure which method the scammers used to get the card information, they said it appears they have had the information for about 8 to 10 months and only recently started using it. Although investigators believe it has been narrowed down to the civic center, they want anyone who has used a card at the Oncenter or War Memorial to also check their statements. Source: http://www.9wsyr.com/mostpopular/story/Civic-Center-credit-card-breach-may-be-a-computer/PSvXYnSEs0WFPp-zCXQf5w.cspx

(Oregon) **FBI seeks local teller in bank fraud probe.** Coos Bay, Oregon police and FBI agents raided the home of a bank teller October 28 with a search warrant. The raid was part of an investigation into charges the suspect stole money from customers' accounts at the Wells Fargo Bank branch at 200 N. Broadway, where she worked. A Special Agent of the FBI's Eugene office said October 29 the suspect eluded arrest October 28, but police and FBI agents are searching for her. According to the FBI Agent's affidavit requesting a warrant from the U.S. Magistrate Judge, the suspect worked at Wells Fargo from August 9, 2006, until August 25, 2010, rising to the position of assistant store manager. She was terminated when Wells Fargo personnel discovered she had opened bank accounts for customers without their knowledge in order to obtain commissions for the new accounts. After the suspect was terminated, two of her regular customers reviewed their accounts and discovered the suspect had made unauthorized withdrawals. Wells Fargo investigators then discovered that using transfers, telephone banking system withdrawals and ATM withdrawals, the suspect had taken as much as $740,000 from the accounts of several customers. Further investigation showed the suspect may have taken as much as $1,200,000 in funds and gold coins from account holders. The affidavit requested a search warrant for digital media, data, financial records, currency, precious metals, and monetary instruments. Source: http://www.theworldlink.com/news/local/article_15dac508-e3f5-11df-a202-001cc4c03286.html

Chemical and Hazardous Materials Sector

(California) **Burglar in Salinas faces health risk after stealing radioactive device.** A burglar's health may be in jeopardy after the thief stole radioactive equipment from a car in Salinas, California police said. A Salinas police spokesman said November 3 that a car burglar had taken a "moisture density gauge" — a type of equipment used to measure moisture in soil — that contains two types of radioactive substances. The potential danger comes only if the device is broken or opened, he said. No immediate problems are expected, but exposure to the substance could lead to cancer in the long run, said the Monterey County health officer. Police said they received a report of the burglary around 8:55 a.m. November 1 on the 400 block of Rainer Avenue. A Troxler 3440 was among the items stolen from a vehicle, the police spokesman said. The gauge was in a yellow case — 18 inches

long, 16 inches deep, and 34 inches wide — with radioactive placards on them. The item weighs up to 40 pounds, police said. Source: http://www.thecalifornian.com/article/20101104/NEWS01/11040309/Burglar-in-Salinas-faces-health-risk-after-stealing-radioactive-device

Commercial Facilities

(Texas) **HPD: Homemade bomb explodes at southwest Houston Walmart.** Houston, Texas police are investigating after a homemade bomb exploded at the front entrance of a Walmart in southwest Houston November 3. Police said someone placed a plastic bottle with a magnesium strip loaded with fluid near the front door of the store located on Kirkwood at Westheimer. The makeshift bomb exploded around 11:30 p.m. The explosion was so loud, an HPD unit driving on the street heard it and rushed to the scene. The HPD bomb squad came out to investigate, but the store was never evacuated. Police said the explosive device was placed in a corner undetectable by surveillance cameras. There were no injuries reported. Source: http://www.khou.com/news/local/Homemade-bomb-explodes-at-southwest-Houston-Walmart-106684938.html

(Virginia) **2 charged in bottle bomb explosions at Mount Trashmore.** An 18-year-old and a juvenile have been arrested in connection with two explosions at Mount Trashmore in Virginia Beach, Virginia, October 30. The bottle bombs went off around 10 a.m. No one was injured. The first explosion occurred when someone threw a 2-liter bottle into a crowd that was gathered for the Harvest Festival. A patron noticed the bottle contents foaming and threw the bottle into a trash can, where it went off. A second bottle bomb exploded near Kids Cove. None of the children playing there were near the site of the explosion. “Bottle bombs can cause some serious injuries — maiming, even blindness could be caused by the solution,” said a fire department official. “And when it discharges in public, it takes the threat to a whole different level, going from a potential prank to nearly reaching domestic terrorism,” he stated. The two suspects were booked November 1, and the case was being screened with the Virginia Beach Commonwealth’s Attorney to determine potential charges beyond manufacturing and use of an explosive device. Source: http://www.wvec.com/news/local/Mount-Trashmore-the-site-of-two-morning-explosions-106372484.html

Communications Sector

(West Virginia) **Copper thieves strike again.** Copper thieves struck again in Kanawha County, West Virginia cutting off phone service to many residents in the Sissonville and Pocatalico areas November 3. The phone lines belong to Frontier Communications. Service was restored late in the evening. Crews from the telecommunications company were in the area repairing the damage for most of the day. A Frontier spokesman said this is the third time since October 28 that thieves have struck the area stealing cable. Source: http://wowktv.com/story.cfm?func=viewstory&storyid=88926

Could a cellphone call from Yemen blow up a plane? A White House counterterrorism adviser said that a pair of bombs shipped to the United States from Yemen were supposed to detonate aboard the airplanes carrying them. The bombs, hidden in printer cartridges, were hooked up to cellphones without SIM cards, the New York Times reported, so calling the phones during intercontinental travel could not have set them off. And experts noted that calling a phone to activate a bomb aboard a plane is one of the least efficient detonation methods. “They couldn’t call,” said a counterterrorism

official from the last two Presidential administrations, now with Goodharbor Consulting. If the terrorists used a regular cellphone to call an airplane-borne bomb from a great distance, it probably would not be able to reach a tower that could bounce a signal to the phone — though it is not impossible. More likely, the official speculated, the bombmakers would have timed the phone's alarm to go off, triggering the bomb. "If they set the alarm, say, two days in advance, and they had confidence how it was shipped and packed to the U.S., then they'd have confidence about where it would be when [it went] boom," he said. A Pentagon adviser who specializes in stopping improvised bombs — and who would only talk on condition of anonymity — cautioned that a satellite phone would have the signal strength to reach the phone packed into the printer-bomb. But keeping that phone ready to receive calls "increases your risk of detection from the device, because you're emitting a signal." Source: http://www.wired.com/dangerroom/2010/11/could-a-cell-phone-call-from-yemen-blow-up-a-plane/

Hacker beats 2G and 3G encryption. Using a simple computer, a home-built transmitter and receiver, plus some readily available software, a developer was able to develop a system whereby he could monitor any conversation using 2G or 3G technology. In the early 1990s came the second generation (2G), which switched from analog to digital transmission, signaling a massive rise in phone usage. The switch to digital also meant that conversations could not be monitored by third parties, due to encryption. Hackers and ham radio enthusiasts had been trying ever since 2G emerged to beat the encryption and now after much experimental work, this developer has managed to crack the system using a device that cost him around 1,000 pounds. Source: http://www.gaj-it.com/26646/hacker-beats-2g-and-3g-encryption/

Android faces critical security study. An analysis of the most critical part of the Android smartphone operating system has turned up programming errors, some of which could allow hackers or malicious applications to access users' e-mail or other sensitive information. The study examined the publicly disclosed version of the Android kernel — heart of Google's open-source software for phones — that shipped inside the HTC Droid Incredible phones. But the study said it is likely other Android phones have the same programming flaws. Android software could be updated wirelessly, so Google would be able to issue the fixes if it confirmed they were needed, a spokesman said. The study by Coverity, the code analysis group, serves as a reminder that smartphones are vulnerable to attacks even as the phones are welcomed more extensively in big companies. Research in Motion, maker of the BlackBerry, and Apple, maker of the iPhone, have also fixed critical security issues in their software through updates. While the number of Android kernel flaws Coverity turned up per 1,000 lines of code is lower than the average for open-source projects, 88 of the Android problems are "high-risk defects". They include improper memory access and memory corruption, and have "significant potential to cause security vulnerabilities, data loss, or quality problems such as system crashes." Source: http://www.ft.com/cms/s/2/10b955ba-e519-11df-8e0d-00144feabdc0.html

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

Joint Japan-U.S. missile defense test flight successful. The Japan Maritime Self-Defense Force (JMSDF) and the United States Missile Defense Agency (MDA) announced the successful completion of an Aegis Ballistic Missile Defense (BMD) intercept flight test, in cooperation with the U.S. Navy, off the coast of Kauai, Hawaii, October 29. The event marked the fourth time a JMSDF ship has engaged a ballistic missile target, including three successful intercepts, with the sea-based midcourse engagement capability provided by Aegis BMD. A separating 1,000 kilometer class ballistic missile target was launched from the Pacific Missile Range Facility at Barking Sands, Kauai, Hawaii. The Japanese vessel detected and tracked the target, then developed a fire control solution and launched a Standard Missile -3 (SM-3) Block IA missile. About 3 minutes later, the SM-3 successfully intercepted the target approximately 100 miles above the Pacific Ocean. Source: http://www.defpro.com/news/details/19370/?SID=a80e06262af1059536d50a1bba8ce6f0

DoD plans 4 new joint helicopters. The Pentagon plans to change the way it buys and develops helicopters and tilt-rotor aircraft in an "as-needed" approach. The approach to purchases and upgrades will be replaced by a "balanced transformational strategy," says the Pentagon's strategic plan for vertical lift aircraft, unveiled August 27 and presented 3 days later to Congress. Pentagon officials also want a significant increase in research and development funds to allow the helicopter industry to develop "next-generation capabilities" for fielding between 2020 and 2050. An annual $110 million boost in science and technology funding is needed to develop technology, to allow military officials to choose between extending the life of the current fleet or buying new aircraft, the plan says. It notes that the military has focused on upgrades to its rotorcraft instead of clean-sheet designs during the past 9 years of war. That trend, plus other "downward trends in science, technology and engineering" in the rotorcraft industrial base, "pose significant risks in addressing the future of DoD requirements," the report says. The answer: develop the "breakthrough technology and new aircraft starts required to achieve next generation vertical lift capabilities." The plan envisions four new "joint multirole" rotorcraft: light, medium, heavy and ultra-sized. The aircraft would be equipped with common systems for situational awareness, avionics, engines, countermeasures and "repairables" that can be used by each service. They would be developed sequentially, with the new technology for each applied to the next, the plan says. Source: http://www.militarytimes.com/news/2010/10/dod-plans-4-new-joint-helicopters-103010w/

Emergency Services

(Florida) **Police substation evacuated by envelope.** The hazardous materials team and bomb squad were called to the Jacksonville Sheriff's Office at Cedar Hills Shopping Center in Jacksonville, Florida, November 3, when a man showed up with an envelope with powder inside. Channel 4 reported that a man opened an envelope with a check and thought it had anthrax inside, so he brought it to the police office on Blanding Boulevard. The area was evacuated until the substance could be analyzed and it was not hazardous. The substation reopened after about 2 hours. The shopping center was never closed. Source: http://www.news4jax.com/news/25620875/detail.html

CBP officer arrested on smuggling charges. A U.S. Customs and Border Protection officer who had fled, apparently to Mexico, in February 2009, was arrested over the weekend of October 30 and 31 on various trafficking charges, court records show. The 38-year-old man was arrested October 30 at B&M International Bridge as he was heading toward Brownsville, Texas according to a press release from the U.S. Attorney's office. He is named in a 13-count indictment from 2009 that charges him

with trafficking, drug trafficking, and bribery. According to the criminal complaint, since August 2005, he allegedly conspired to bring undocumented immigrants into the country by using his official capacity as a government official for financial gain. From November 2007, he is accused of conspiring to use his official capacity to bring kilogram quantities of cocaine into the country. The case was investigated by the U.S. Immigration and Customs Enforcement Office of Professional Responsibility, the FBI, CBP Internal Affairs, and the DHS Office of the Inspector General. Source: http://www.brownsvilleherald.com/articles/arrested-118898-charges-officer.html

(Washington) **Prison evacuated after suspicious device found.** A suspicious device found in a living area at the Airway Heights Corrections Center in Airway Heights, Washington prompted an evacuation of inmates and staff November 1. The Spokane County bomb squad and hazmat team responded and removed a can with a paper wick, according to a press release. There was a small amount of mineral oil in the can. The minimum-security facility houses 600 inmates. Source: http://www.spokesman.com/stories/2010/nov/02/prison-evacuated-after-suspicious-device-found/

(West Virginia) **Fibernet to develop notification procedures.** Fibernet officials said they will work to develop procedures for notifying emergency officials when it has a widespread outage in West Virginia. The company experienced two service interruptions in October 2010. Customers across the state lost telephone and Internet service for about 4 hours October 25. Another outage occurred in at least six counties October 10. The Charleston Gazette reported the state public service commission is investigating Fibernet's recent outages. Fibernet said it does not provide service to emergency services centers in West Virginia, but its customers include first responders such as the Charleston Fire Department. The Kanawha County Commission president said Fibernet must notify 911 centers in a timely manner when service is interrupted. Source: http://www.wtap.com/news/headlines/Fibernet_To_Develop_Notification_Procedures_106303788.html?ref=788

(New Jersey) **Lawmakers call for a clear emergency signal for New Jersey.** Politicians and various branches of the Gloucester County, New Jersey emergency response team rallied October 29 to call for the Federal Communications Commission to intervene in new digital television signals that interfere with emergency communications frequencies. Broadcast stations from North Carolina, Connecticut and Massachusetts are being influenced by an atmospheric condition called Tropospheric Ducting, in which a digital signal gets trapped in a duct of cold air being overrun by warm air. Most common during periods of stable, anticyclonic weather, authorities said the summer and autumn months create ideal conditions for this phenomenon, with temperature inversions occurring most frequently along coastal areas bordering large bodies of water. The broadcast signal gets trapped within these ducts created by overlapping channels of air, and follows a path sometimes up to 250 miles away, where it drops into and begins interfering with other signals carried on the same wavelength to which the DTV signal is broadcast. The digital signals are supposed to be restricted to a 50-mile radius based on their signal strength, but these air ducts cause them to travel much farther. As a result, radio signals between dispatch and emergency response teams such as the police and fire departments and EMS squads will become scratchy, garbled, or cut out altogether when these signals drop into the channel. Source: http://www.nj.com/gloucester/index.ssf?/base/news-6/1288427128298280.xml&coll=8

Energy

Hackers tap SCADA vuln search engine. A search engine that indexes servers and other Internet devices is helping hackers to find industrial control systems that are vulnerable to tampering, the US Computer Emergency Readiness Team (US CERT) has warned. The 1-year-old site known as Shodan makes it easy to locate Internet-facing SCADA, or supervisory control and data acquisition, systems used to control equipment at gasoline refineries, power plants, and other industrial facilities. As white-hat hacker and Errata Security CEO explained, the search engine can also be used to identify systems with known vulnerabilities. According to the Industrial Control Systems division of US CERT, that is exactly what some people are doing to discover poorly configured SCADA gear. "The identified systems range from stand-alone workstation applications to larger wide area network (WAN) configurations connecting remote facilities to central monitoring systems," the group wrote in an advisory (PDF) published October 28. "These systems have been found to be readily accessible from the internet and with tools, such as Shodan, the resources required to identify them has been greatly reduced." Besides opening up industrial systems to attacks that target unpatched vulnerabilities, the data provided by Shodan makes networks more vulnerable to brute-force attacks on passwords, many of which may still use factory defaults, CERT warned. Source: http://www.theregister.co.uk/2010/11/02/scada_search_engine_warning/

Food and Agriculture

(New York) **Expansion of New York Gourmet Salads, Inc. recall.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) is expanding its October 30 public health alert for an undetermined amount of various meat and poultry products produced without the benefit of federal inspection by N.Y. Gourmet Salads Inc., a Brooklyn, New York establishment. This public health alert was initiated based on evidence collected during an ongoing investigation being conducted by FSIS involving this establishment. Additional products subject to this expanded alert include, but are not limited to, the following: 4.5-pound and 5-pound containers of "Lemon Grilled Chicken"; 5-pound containers of "Grilled Chicken"; 4.5-pound and 5-pound containers of "Breaded Chicken"; 6-pound containers of "Stuffed Cabbage"; 5-pound containers of "Grilled Chicken, Plain"; 5-pound containers of "Teriyaki Grilled Chicken"; and 5-pound containers of "Chopped Chicken Liver." The implicated products were produced between April 20 and October 29, and were distributed to retail establishments in New York. Source: http://www.foodpoisonjournal.com/2010/11/articles/food-poisoning-watch/expansion-of-new-york-gourmet-salads-inc-recall/

(Vermont) **High Neomycin levels found in Vermont veal calves.** The prescription animal drug Neomycin is an antibiotic that kills bacteria rapidly by suppressing protein synthesis and growth. The U.S. Food and Drug Administration (FDA) tolerance level is 7.2 parts per million (ppm) for Neomycin in the kidneys of cattle. Health officials fear that when antibiotics like Neomycin get into the food supply at higher levels, the practice could contribute to humans building up resistance to commonly prescribed antibiotics. That is why FDA regulates the use of drugs in animal agriculture. On a recent inspection of Vermont's Longway Farm, located near Swanton, FDA found Bob veal calves being sold for slaughter as food with higher than tolerated levels of Neomycin. In an October 5 warning letter to Longway Farm, FDA said the animals the dairy was offering for sale were adulterated because of the improper use of animal drugs. Three Bob veal calves sold on March 15 and 29, and slaughtered the next day, were found with 17.25 ppm; 21.58 ppm; and 8.25 ppm of Neomycin in their kidney tissues.

The U.S. Department of Agriculture's Food Safety and Inspection Service conducted the tissue analysis. Source: http://www.foodsafetynews.com/2010/11/vermont-veal-calves-found-with-high-neomycin-levels/

(New York; New Jersey) **Nova Lox Salad recalled due to Listeria.** A lox salad sold at Costco stores in New York and New Jersey has been recalled after health inspectors found the product to be contaminated with Listeria, the U.S. Food and Drug Administration reported October 29. Tuv Taam Salads Nova Lox Salad was recalled by Kosher First LLC after routine sampling by New York State Department of Agriculture and Markets Food Inspectors and subsequent analysis found the product to be positive for Listeria monocytogenes. The salad should not be eaten. Source: http://www.foodsafetynews.com/2010/10/lox-salad-recall/

(New York) **Alert issued for uninspected food in New York.** The U.S. Department of Agriculture's (USDA's) Food Safety and Inspection Service (FSIS) has issued a public health alert for various meat and poultry products prepared by a Brooklyn, New York, company, saying the food did not undergo federal inspection. The USDA said the alert for certain foods produced by N.Y. Gourmet Salads Inc., was initiated "based on evidence collected during an ongoing investigation." Evidence showed the establishment had been distributing produce without federal inspection, the agency said. The USDA said products subject to the alert include, but are not limited to, the following: 5-pound tubs of "Chicken Salad," and 5-pound trays of "Meatballs & Sauce," "Meatballs," "Swedish Meatballs," and "Sausage & Pepper." The products were produced between March 11, 2010 and October 29, 2010 and were distributed to retail establishments in New York. Source: http://www.foodsafetynews.com/2010/11/warning-issued/

Government Sector (including Schools and Universities)

(Ohio) **Authorities: Licking County man found with pipe bomb threatened courthouses.** Authorities said a Licking County, Ohio, man arrested October 27 after he crashed into a church while fleeing law enforcement officers, had threatened to place bombs at county court buildings. The 35-year-old suspect, of Newark, was arrested after he struck the cruiser of a deputy sheriff who tried to serve him with a warrant for failure to pay child support. He then led officers on a chase from the Newark motel where he was staying to a church on Jacksontown Road, south of the city, where he crashed his vehicle. Inside his van, police found a working pipe bomb that was later neutralized by the Franklin County sheriff's bomb squad. In a subsequent search of the vehicle this week, detectives found evidence that suggested the suspect had either placed or intended to place a second bomb at a Licking County courthouse, a captain said. Source: http://www.dispatch.com/live/content/local_news/stories/2010/11/03/Licking-County-bomb-threat.html?sid=101

Concerns over leftwing extremists. In advance of the historic midterm Congressional election that swept conservatives, moderates, and fundamentalist constitutionalists into power November 2, a disturbing "surge of intelligence" began to warn of a possible threat from ultra-leftwing extremist groups and individuals should Democrats and liberals lose one or both chambers of Congress, according to counterterrorism officials who spoke to HSToday.us. The intelligence is in glaring contrast to concerns by largely partisan groups and organizations this past year that dwelled on fears

that extremist rightwing elements pose the greatest homegrown domestic terrorism threat. The officials said intelligence indicates some may be planning to engage in terrorist acts in response to the significant gains made in Congress by Republicans, Independents, and "conservatives in general." Source: http://www.hstoday.us/content/view/15310/150/

(Virginia) **FBI: Gunfire at Virginia recruiting center linked to other incidents.** Ballistic tests have linked a shooting at a Coast Guard recruiting office in Virginia to four other shootings at military facilities last month, the FBI said November 3. The latest incident was reported November 2 after a bullet struck the recruiting office, housed in a Woodbridge strip mall. The description was "relatively similar" to October cases in which shots were fired at the Pentagon, the National Museum of the Marine Corps, and a vacant Marine recruiting station, said a spokeswoman for Prince William County police. No one has been injured in any of the incidents, including when six shots were fired at the Pentagon October 19. Source: http://www.cnn.com/2010/CRIME/11/03/virginia.military.shooting/index.html?hpt=T2

(New Jersey) **University accidentally emails personal student data.** Seton Hall University in New Jersey has inadvertently e-mailed an Excel spreadsheet with the personal and educational information of 1,500 seniors to 400 other students. It seems that the document, which contained the names, addresses, e-mails, student ID numbers, majors, credit hours, and grade-point averages of students identified as seniors got attached to the e-mail by mistake. The interim provost later sent another e-mail entitled "Security Incident," advising the 400 unintended recipients not to open, view, forward, send, discuss or distribute the spreadsheet. According to the Setonian, the university has launched an investigation into the breach and apologized for the error. It expressed commitment to take the necessary precautions in order to ensure the safety of the exposed accounts. Source: http://news.softpedia.com/news/Seton-Hall-University-Emails-Personal-Student-Data-Accidentally-164371.shtml

(Mississippi) **Weekend shooting prompts Newton school district to add more security at prep football field.** A shooting in the parking lot of Newton High School in Newton, Mississippi, during a football game October 29 has prompted officials to take steps to add security. Police said the shooting was not game-related, it did not involve any students, and no one in the stadium was hurt. Police said one person was wounded, but no arrests have been made. The school's superintendent said the school board is looking at ways to limit access, increase lighting, and increase security. She said the grassy field, which serves as the football field's parking lot, is located next to a county road. School officials now plan to enclose the entire field in a chain-link fence. The superintendent said the area is too large for the school system to hire more security to patrol it. Source: http://www.wreg.com/news/sns-ap-ms--newtonschools,0,588802.story

(Georgia) **Bomb warning led to courthouse sweep.** Fulton County, Georgia, authorities said they were forced to sweep the downtown courthouse complex for explosives November 1 after receiving a threat warning that a device in the building would explode at 1 p.m. A sheriff's spokeswoman said more than a dozen agencies, some armed with bomb-sniffing dogs, inspected the three-building complex after the threat was received around 10:30 a.m. The complex was not evacuated, but authorities asked everyone to remain in their offices, and streets outside the building were closed. Authorities reopened the courthouse at 12:42 p.m. after it was deemed safe. Source: http://www.sfexaminer.com/local/ap/fulton-courthouse-receives-bomb-scare-106453318.html

(Virginia) **Shots fired at Coast Guard recruiting station in Woodbridge.** Police are investigating a report of shots fired into a Coast Guard recruiting station in Woodbridge, Virginia, the fifth overnight shooting at a Northern Virginia military facility since October 17. The shots were discovered early November 2, said a Prince William County police spokeswoman. No one was injured, she said. The recruiting station is near the Potomac Mills mall. Police and the FBI are probing four other similar shootings — two at the National Museum of the Marine Corps, one at the Pentagon, and one at a Chantilly Marine Corps recruiting station. The same weapon was used in at least three of those shootings, and FBI officials said they believe the gunman is someone who has a grievance against the Marines, but who is not trying to hurt anyone. Source: http://www.washingtonexaminer.com/local/blogs/capital-land/shots-fired-at-coast-guard-recruiting-station-in-woodbridge-106517918.html

(Nevada) **Cosmetology school in Reno evacuated.** The Milan Institute of Cosmetology in Reno, Nevada, was evacuated October 29 after a woman allegedly made threats toward people inside. It happened just before 2 p.m. on Matley Lane. Reno police said a woman showed up and made threats to those inside. A witness told KRNV News 4 the woman even made a threat to shoot people inside. Police would not release much information, but said the woman appeared to have mental health issues. Officers said the woman kicked an officer, before she was arrested and taken to jail. No one else was injured in the incident. Source: http://www.mynews4.com/story.php?id=30781&n=122

Napolitano: Military to aid civilian cybersecurity. The Defense Department's National Security Agency (NSA) can be used "appropriately" on civilian cybersecurity matters, the Homeland Security secretary said October 28. She said that an agreement between the military and DHS, announced in October, takes privacy and civil liberties into account. The agreement allows DHS to tap into NSA expertise on cybersecurity issues. She said her department and the military are responsible for 95 to 99 percent of the federal jurisdiction for cybersecurity, so a partnership was logical and necessary to make the most of both departments' resources and expertise. The Secretary did not elaborate on what the NSA's role in civilian cybersecurity would be. Source: http://topnews360.tmcnet.com/topics/associated-press/articles/2010/10/31/112919-napolitano-military-aid-civilian-cybersecurity.htm

(Virginia) **DC-area gunman may have grievance against Marines.** A gunman who fired shots at a Washington-area Marine Corps museum and is believed to be responsible for three similar incidents may have a grievance against the U.S. Marine Corps, the FBI said October 29. The acting assistant director for the FBI's Washington field office said during a press conference that investigators believe the person takes issue with the institution of the Marines, but not those serving in uniform. The person has made sure no one has been hurt, and authorities do not believe he wants to harm citizens or Marines. he said. The suspect may be dealing with a traumatic event such as loss of a job, financial problems, or divorce. The acting assistant director said officials are working under the assumption that the individual was part of the Marine Corps. The FBI has said the first three shootings are connected, and investigators say they assume the fourth is connected as well.Source: http://topnews360.tmcnet.com/topics/associated-press/articles/2010/11/01/113051-dc-area-gunman-may-have-grievance-against-marines.htm

Information Technology and Telecommunications

PC typing errors can help guard against intruders. Japan's NTT Communications has developed a computer security system that analyzes the way a computer user types, and then checks it against a profile of authorized users to detect if the person at the keyboard is an imposter. The system, called Key Touch Pass, records the speed at which a user is typing, the length of time they typically hold down each key and the errors they normally make. Every few hundred characters it checks this against a profile of the user that is supposedly logged in to the computer. If the two differ by more than a predetermined threshold, the system concludes the computer's user isn't who it should be. NTT Communications anticipates the system could have uses beyond security and has already conducted trials with e-learning networks. Distance learning systems rely on the honesty of users, especially when taking online tests. The company is also eyeing potential use in the online banking field. During a demonstration of the system, which works in both Japanese and English, it was able to detect an imposter after several lines of text had been typed. Source: http://www.computerworld.com/s/article/9194859/PC_typing_errors_can_help_guard_against_intruders

Malware writers step up AutoRun attacks. Anti-virus firm Avast Software has warned of a growing risk to enterprise systems from infected USB devices targeting the AutoRun feature in Windows. The company said one in eight of the 700,000 attacks recorded by the firm's CommunityIQ system came from USB devices. "The threat of USB-distributed malware is much more widespread than just the Stuxnet attacks on enterprise computers, which were also spread via infected memory sticks," said an Avast Virus Lab analyst. "Cyber criminals are taking advantage of people's natural inclination to share with their friends, and the growing memory capacity of USB devices. Put these two factors together and we have an interesting scenario." Once infected with a generic USB worm, detected by Avast as 'INF:AutoRun-gen2 [Wrm]', an executable file is started which then allows a wide variety of malware to copy itself into the core of Windows. The malware then replicates each time the computer is started. "This danger is poised to increase with the introduction of the new USB 3 standard," he said. Source: http://www.v3.co.uk/v3/news/2272718/avast-autorun-windows-malware

Researchers to demonstrate new attack that exploits HTTP. A flaw in the HTTP protocol leaves the door open for attackers to wage a new form of distributed denial-of-service (DDoS) attack that floods Web servers with very slow HTTP "POST" traffic. Researchers at the upcoming OWASP 2010 Application Security Conference will demonstrate the new attack, showing how online gaming could be used as a way to recruit bots in an "agentless" botnet that executes the attack. The bot does the bidding of the botnet without getting infected with bot malware. The researcher who first discovered the attack in 2009 with a team of researchers in Singapore, said HTTP is "broken" and leaves all Web-based servers or systems with a Web interface vulnerable to this form of attack. "This talk is very sensitive and should be highlighted for U.S. critical infrastructure," the researcher said of his upcoming presentation. "If it has a Web interface, we can knock it down [with this attack]: think SSL VPN and other critical systems accessed with a Web browser that you need to connect to by posting information." It could be used to take down any HTTP or HTTP-S service — including some supervisory control and data acquisition (SCADA) systems. "Internal clients can be exploited to launch the slow HTTP POST attacks to the SCADA systems via authorized HTTP connections and from authorized clients," he said. "One does not need millions of connections to bring down a Web server." Source:

http://www.darkreading.com/vulnerability_management/security/attacks/showArticle.jhtml?articleID=228000532

Computer scientist creates new way to combat hacking. In the fight against malicious hackers, a Virginia Polytechnic Institute and State University (Virginia Tech) professor said she has created a new weapon to fend off malware. The assistant professor of computer science said she has developed a framework to combat "spoofing attacks." A spoofing attack is when organized botnets — groups of computers that are controlled by malicious software — run by hackers, are able to penetrate someone's computer and steal their identity. These attack bots are able to do this by emulating a user's keystroke sequences. The assistant professor holds a patent on her human-behavior-driven malware detection technology. The professor and her colleague, now a graduate student in the computer science department at Stanford University, have developed a system to combat these attacks. Called "Telling Human and Bot Apart" (TUBA), it is able to differentiate when the bot and human are typing. It is based on a remote biometrics system. It also uses a cryptographic mechanism that prevents the bot from pretending to be human. Source: http://www.ibtimes.com/articles/77893/20101102/tech-malware-hacking-virginia-tech-hackers-computer-security.htm

Aviation chief calls for security overhaul. Outdated security systems introduced to combat airliner hijacking 40 years ago must be overhauled to address new terrorism threats, the head of the International Air Transport Association (IATA) said November 2. "Today's threats require a different approach and different technology," IATA's director-general told delegates atthe AVSEC aviation security conference in Frankfurt, Germany. His comments came 4days after authorities in the United Arab Emirates and Britain found two packages sentfrom Yemen believed to contain the explosive material PETN. "The events in Yemen have put cargo security at the top of our agenda," the official said, pointing out that 35 percent of goods traded worldwide are shipped by air, which in 2009 amounted to som26 million tons. "Transporting these goods safely, securely and efficiently is critical," he said, emphasizing that the responsibility for that should not just fall on airlines, but "the entire supply chain, from manufacturer to airport," driven by co-operation betweegovernment and industry. Source: http://www.cnn.com/2010/WORLD/europe/11/02/aviation.cargo.security/

Student creates tool to fight Facebook hacking on WiFi. A student at the University of Iceland has programmed a potential antidote to Firesheep, a hacking tool that can access social networking accounts over unsecured WiFi networks. It is called FireShepherd and it aims to stop Firesheep, which was apparently created with good intentions but has the potential to wreak havoc. A Seattle-based software developer released Firesheep as a way of informing Internet users about the dangers of using public WiFi networks that are not password protected. Hackers have long been able to intercept data that crosses open WiFi networks, but Firesheep makes it simple for virtually anyone to do it. The Icelandic student said FireShepherd is a way to protect against Firesheep while using public WiFi; it will also guard the other users on the same network. He said the program floods the network with data that should stop Firesheep from working. But he warns that FireShepherd will not protect against other more-sophisticated hacking methods, and users should still be cautious about what they do on a public network. Source: http://www.thestar.com/business/article/883046--student-creates-tool-to-fight-facebook-hacking-on-wifi

(Virginia) **IT director gets jail term for hacking former employer's site.** A man fired as IT director for a Richmond, Virginia, seller of telecom equipment has been sentenced to 27 months in prison for hacking into his former employer's Web site and deleting files, the U.S. Department of Justice (DOJ) said. The convict pleaded guilty to one count of intentionally damaging a protected computer without authorization June 29. He was sentenced October 29 in U.S. District Court for the Eastern District of Virginia and, in addition to the prison time, he was ordered to pay $6,700 in restitution to Trans Marx, which sells discounted telecom equipment and supplies. The convict, of Richmond, worked at Trans Marx from February to June 2008, according to court documents. Before he was fired, he had access to the Trans Marx computer network, including the company Web site hosted in Georgia, the DOJ said. On July 25, the convict used a personal computer and an administrator account to access the computer hosting the company's Web site, and he deleted about 1,000 files related to the Trans Marx site, the DOJ said. Source: http://www.computerworld.com/s/article/9194027/IT_director_gets_jail_term_for_hacking_former_employer_s_site

RIAA and Anonymous sites both downed by DDoS assaults. Hacktivists briefly took out the two main Recording Industry Association of America (RIAA) Web sites October 29 as revenge for the organization's long-running legal offensive against Limewire, which led to the closure of the controversial P2P service earlier in the week. Denizens from the loosely-affiliated Anonymous collective used its Low-Orbit Ion Cannon (LOIC) tool to swamp the Web sites of RIAA.org and RIAA.com with spurious traffic. The assault began around 5 p.m., Slyck.com reported. The assault was originally coordinated from the Operation Payback site (http://tieve.tk), which helped coordinate an ongoing series of distributed denial of service (DDos) attacks against entertainment industry Web sites that began last month. The campaign is designed to support The Pirate Bay and came in response to the Bollywood film industry's use of hired guns prepared to launch DDoS attacks against file-sharing sites in cases where legal action failed to bear fruit. However, after tieve.tk itself came under attack, the attackers moved shop to anonops.net. Service to tieve.tk has largely been restored. The riaa.com and riaa.org sites remained unavailable from Europe, possibly as a deliberate defensive measure aimed at containing the latest in a long line of hack attacks against RIAA. Source: http://www.theregister.co.uk/2010/11/01/riaa_anon_ddos/

Facebook hits developers that passed user IDs to data broker. Facebook is punishing several application developers for passing certain information to a data broker in the latest move by the social networking site to control growing concerns over privacy. Facebook will deny those application developers access to "communication channels" for 6 months, wrote a spokesman, on Facebook's blog, October 29. The developers number fewer than a dozen, he said. The developers were being paid by a data broker for user IDs, unique numerical identifiers assigned to the site's users, which can appear in a URL when they use the site. After an investigation into online privacy by the Wall Street Journal, Facebook said last month that in some cases user IDs were inadvertently being passed on to applications, which is against Facebook's policy. The situation was due to a Web standard called referral URLs that lets a Web site know where a person was previously browsing. The user IDs do not contain personal information, but could lead to information that the person has chosen to display publicly. The latest revelation, however, shows that some application developers were then passing those user IDs to a data broker. Those brokers typically compile information to sell to advertising networks so users can be targeted with ads that are related to their personal interests. Source:

http://www.computerworld.com/s/article/9194199/Facebook_hits_developers_that_passed_user_IDs_to_data_broker

National Monuments and Icons

(Virginia) **Firefighters battle wildfire in Page County.** Falling leaves are hampering efforts to extinguish a wildlife that has burned almost 400 acres in the George Washington National Forest in Page County, Virginia. The Daily News-Record reported that firefighters set fire to about 182 acres October 31 in an attempt to prevent the blaze from spreading. The fire on the eastern slope of the Massanutten Mountain range was reported October 24. It was 60 percent contained October 31. A U.S. Forest Service spokeswoman said falling leaves are the biggest problem. The cause of the fire has not been determined. Source: http://www.wset.com/Global/story.asp?S=13421464

Postal and Shipping

(California) **Menifee man finds 'suspicious white powder' in envelope; authorities investigate.** Sheriff's investigators are looking into a suspicious envelope containing a white powder that was delivered to and opened by a Sun City, California man November 3, said a police spokesman. The man who opened the envelope did not display any medical problems, said the spokeswoman for the Riverside County Sheriff's Department. The incident was called in about 6:55 p.m. in the 26800 Maris Court area, near Murrieta Road in the Sun City area of Menifee, the spokesman said. The man received the envelope and opened it before seeing a white powder inside, prompting him to call authorities. The spokesman said there have been no evacuations and the hazardous material team is handling the incident, along with sheriff's investigators. Source: http://www.swrnn.com/southwest-riverside/2010-11-03/news/menifee-man-finds-suspicious-white-powder-in-envelope-authorities-investigate

(New York) **J.F.K. airport cargo area evacuated after package is found.** A cargo area at John F. Kennedy International Airport in Queens, New York was briefly evacuated November 3 when a suspicious package from Yemen was discovered, authorities said. The package, found in a DHL Express cargo area about 5:30 p.m., contained a cellphone, officials said. The discovery prompted concern because it came 1 week after authorities foiled a plot in which two separate bombs — each containing circuit boards from cellphones — were sent from Yemen to Chicago via FedEx and U.P.S. Those packages were intercepted before reaching the United States. The discovery of the package November 3 led to the evacuation of the DHL cargo facility out of an abundance of caution, said a FBI spokesman. The package was determined safe just after 8 p.m., and workers were allowed to return. The evacuation did not affect any passenger terminals, a Port Authority spokesman said. Source: http://www.nytimes.com/2010/11/04/nyregion/04evacuation.html?_r=1

U.S. suggests measures for cargo security. Top-level U.S. security leaders November 3 communicated directly with officials of the major all-cargo and express air carriers and visited Yemen, the country believed to be the source of last week's printer bomb threats. The Homeland Security Secretary discussed enhanced security measures with officials at UPS, DHL, FedEx, and TNT, and suggested preventative measures that would include terrorism awareness training for their employees, who number about 1 million. In a talk with the director general of the International Air Transport Association (IATA), she underscored the partnership with airlines and alliances that focuses on

layered security. An IATA spokesman said the industry group was pleased that the secretary "reached out to the industry." At a security conference in Frankfurt, Germany this week, the IATA chief also met with the director of the Transportation Security Administration. Source: http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aviationdaily&id=news/avd/2010/11/04/05.xml

(Georgia) **Gov't building evacuated after white powder scare.** Police and firefighters have issued an all-clear after a hazmat situation prompted the evacuation of an Atlanta, Georgia government building November 2. Someone mailed an envelope containing a small amount of white powder to the Sloppy Floyd building. There was so little powder that officials said they could not detect the contents at the scene. The envelope and contents were taken to an area crime lab for further testing. The call came in at about 4 p.m., prompting the building's west tower to be evacuated, said a spokeswoman for the Georgia Building Authority. Four people were isolated and evaluated during the ordeal, police said. Homeland Security was also notified of the incident, police said. Piedmont Avenue was shut down from Martin Luther King to Decatur while the investigation continued. Source: http://www.wsbtv.com/news/25609520/detail.html

(Oregon) **FBI: Suspicious items found on flight into PDX.** A flight to Portland, Oregon that originated in Tokyo, Japan had suspicious, but non-explosive items on board, according to the FBI. The crew of Delta Flight 90 "opted to contact authorities and request they meet the aircraft upon arrival as a result of some box cutter blades found onboard while the aircraft was enroute," according to Delta Airlines. The 154 passengers and 10 crew members were interviewed November 2 at Portland International Airport, said an FBI spokeswoman. Flight 90 originates in Seoul, South Korea according to the airline Web site. Source: http://www.kgw.com/home/FBI-detains-Delta-passengers-at-PDX-on-flight-from-Tokyo-106535433.html

Mail under scrutiny. U.S. issues advisory. The FBI and Homeland Security Department have cautioned that foreign-origin packages without return addresses and excessive postage require a second look, according to an advisory sent to local officials around the country that was obtained November 1 by the Associated Press. And Germany's aviation authority extended its ban on air cargo from Yemen to include passenger flights. Britain banned the import of larger printer cartridges by air November 1 as it also announced broader measures to halt air cargo from Yemen and Somalia following the ink cartridge bomb plot. Yemeni authorities November 1 continued to hunt for suspects tied to the mail bomb plot, but a young woman arrested soon after the attacks were thwarted was released. Investigators there said someone had stolen her identity and used it to mail the package. Source: http://www.ohio.com/news/nation/106501208.html

(Alabama) **Resident finds white powder.** Hazardous materials experts were called to a Lawrence Avenue home in Florence, Alabama, October 30 after one of the residents opened an envelope containing a white powdery substance wrapped in plastic. Law enforcement officials were expected to analyze the substance, according to the Lauderdale County Emergency Management Agency (EMA) director who responded to the scene along with Florence police and firefighters. The Colbert County EMA director also responded to the call. The residents did not come in contact with the substance in the envelope. "The main thing I would want people to know, if you get something like this, do like these people and don't shake it out into the air," the director said. Anyone receiving similar packages should contact law enforcement authorities immediately, he said. Source:

http://www.timesdaily.com/article/20101031/NEWS/101039979?Title=Resident-finds-white-powder-

Feds warn local law enforcement about more possible mail bombs. Counter terrorism officials are warning local law enforcement and emergency personnel to be on the lookout for mail that could have dangerous substances hidden inside. The FBI and Homeland Security Department said packages from a foreign country with no return addresses and excessive postage need to be scrutinized, according to an advisory sent to local officials around the country and obtained November 1 by the Associated Press. Mail bombs believed to have been designed by the top explosives expert working for al-Qaida in the Arabian Peninsula were sent in packages addressed to Jewish synagogues last week. While officials caught two bombs in the United Arab Emirates and the United Kingdom, U.S. officials said there may be more in the system. Source: http://www.foxnews.com/us/2010/11/01/feds-warn-local-law-enforcement-possible-mail-bombs/

U.S. nuclear-bomb scan ignored by truckers, boxes go unchecked. Two years after South Korea's busiest port installed a $3.5 million scanner to check U.S.- bound shipping containers for nuclear weapons, the machine sits idle because truckers will not drive through it due to fears of radiation exposure. That means about 1.9 million containers left Busan for American harbors last year without U.S.-mandated screening. Singapore and Hong Kong, the world's busiest and third-busiest ports, also do not participate. Nine years after the September 11 attacks, less than 1 percent of the 14.5 million cargo boxes reaching U.S. shores are scanned abroad, the government said. A goal to screen all containers is opposed by the Retail Industry Leaders Association, a group representing Wal-Mart Stores Inc., Apple Inc., and Nike Inc. "Prohibitive challenges" involving cost and technology mean a July 1, 2012, deadline for 100 percent inspections will be delayed by at least 2, the DHS Secretary said. "The system remains very vulnerable," said the president of the Washington-based Center for National Policy, which studies security issues. "If I were an adversary who wants to cause mass destruction to the global economy, this is the system to target." Source: http://www.bloomberg.com/news/2010-10-30/u-s-nuclear-bomb-detector-ignored-by-truckers-leaves-shipping-vulnerable.html

PUBLIC HEALTH

Power infrastructure lacks reliability in many US hospitals. Many IT managers and IT operations professionals in U.S. hospitals are not adequately informed about the importance of power infrastructure strategies, while reliance of the sector on IT continues to grow, concluded a survey conducted by Emerson. The 2010 survey on IT and facility issues in hospitals questioned North America-based IT management and IT operations professionals, as well as data center and facilities managers. More than half of respondents said they had upgraded their facilities' power and cooling infrastructure as they implemented new technologies like VoIP, network communications, picture archiving, and communication systems. The importance of uninterruptible power supply (UPS) for hospital facilities is apparently not as well understood as its importance in data centers and network closets. More than half of patient rooms are not supported by a source of uninterruptible power, according to the release, and only 28 percent of operating rooms have emergency power receptacles serviced through a UPS. Source: http://www.datacenterdynamics.com/ME2/dirmod.asp?sid=&nm=&type=news&mod=News&mid=9A02E3B96F2A415ABC72CB5F516B4C10&tier=3&nid=FDECA003F2734F8589AEA59DDF1E8595

(Delaware) **Two bomb threats, an hour apart, keep State Police busy.** Delaware State Police troopers are investigating bomb threats that were called in to two separate locations November 1. The first incident occurred at about 2:50 p.m. when a male called the Rite Aid Pharmacy in New Castle and spoke to the pharmacist. He said he had placed a bomb inside the store, inside each store employee's car, and inside each store employee's home. Two police canines specifically trained in bomb detection and their handlers responded to the scene and conducted a search of both the interior and exterior of the store. No devices were located and the store was re-opened for business. At 3:45 p.m. troopers responded to the Emily P. Bissell Hospital located in Wilmington in reference to a bomb threat called in at that location. A state police bomb-trained canine and his handler then responded to the hospital and conducted a search of the exterior. No device was located. The hospital was not evacuated. Source: http://www.newarkpostonline.com/articles/2010/11/01/news/doc4ccf502817dc6972230032.txt

Continuing drug shortages affect North American patients. Pharmacists across Canada said drug shortages are affecting patients and will likely continue to do so, despite assurances from manufacturers that they are trying to increase supplies. The association in October surveyed members about whether they were unable to fill any prescriptions during their most recent shifts, and over the previous week. Of the more than 600 pharmacists who responded online, 84 percent had problems locating a drug during their most recent shift, and 94 percent could not find at least one drug in the previous week. The 89 percent of pharmacists also said that drug shortages have greatly increased over the past 12 months, while 70 percent said the shortages were affecting their patients' health. The United States Food and Drug Administration (FDA) lists more than 40 drugs in short supply. An FDA official said most of those are sterile injectable products, which are "on the brink" of being unavailable. American patients have been affected by some shortages, including a critical lack this summer of propofol, an injectable anesthetic, she said. That particular shortage occurred when two of the three firms that make propofol in the United States had quality issues, including one with a risk of microbial contamination. Source: http://www.cmaj.ca/earlyreleases/1nov10-continuing-drug-shortages-affect-north-american-patients.dtl

TRANSPORTATION

Mail bombs may have been planned to explode in mid-flight. The mail-bomb plot stretching from Yemen to Chicago may have been aimed at blowing up planes in mid-flight and was only narrowly averted, officials said October 31, acknowledging that one device almost slipped through Britain, and another seized in Dubai was unwittingly flown on two passenger jets. Senior U.S. officials met to develop a U.S. response to the al Qaeda faction linked to the powerful explosives addressed to synagogues in Chicago that would have gone via Philadephia. Investigators were still studying the two bombs they believed were designed by the top explosives expert working for al Qaeda in the Arabian Peninsula, the Yemen-based militant faction thought to be behind the plot. Yemeni authorities released a woman engineering student arrested earlier, saying someone else had posed as her in signing the shipping documents. Authorities admitted how close the terrorists came to getting their bombs through, and a senior U.S. official said investigators were still trying to figure out if there were other devices in the pipeline. Source:

http://www.philly.com/dailynews/national/20101101_Mail_bombs_may_have_been_planned_to_explode_in_mid-flight.html

Airlines required to provide new passenger information to TSA. As of November 1, U.S. airlines must collect new personal information from passengers, as it appears on government-issued ID, before they board a flight. A new Transportation Security Administration (TSA) rule mandates airlines to collect a passenger's full name, date of birth, and gender. "If you don't provide the information, it's pretty simple — you can't complete your reservation, you can't get a boarding pass, and you can't travel," a spokesman said for the Air Transport Association. The industry association represents all major U.S. airlines. The TSA program, called Secure Flight, has been implemented in phases since late last year. The rule came as a result of a 9/11 Commission recommendation made 6 years ago. It is geared towards improving aviation safety, and providing consistency in the airline industry's identification matching process. Source: http://marketplace.publicradio.org/display/web/2010/11/01/am-airlines-required-to-provide-new-passenger-information-to-tsa/

Bomb plot shows gaps in screening of air cargo. The Transportation Security Administration (TSA) boasted that every piece of cargo carried on domestic passenger flights is screened for bombs before being put in the belly of an airliner. However, when it comes to ensuring the security of cargo packages on foreign flights heading to the United States, the TSA makes no such proclamations. Despite federal law requiring all cargo on U.S.-bound passenger flights to be screened as of August 2010, authorities still are not close to meeting the requirement. A reminder of that gap in airline security — and of the daunting challenge officials face in closing it — came last week, when terrorists in Yemen linked to al-Qaeda slipped bombs into cargo packages addressed to synagogues in Chicago. The discovery of the explosives in cargo shipments at airports in northern England and Dubai reflected how the complexities in shipping cargo by air can leave passengers on commercial airliners vulnerable to such security breaches: By the time the explosives were detected, both shipments had made part of their journey from Yemen on passenger jets. That is why investigators are trying to determine whether the Yemen plot was about sending explosives to the USA, blowing up cargo jets, or even trying to attack passenger jets that happened to pick up the packages from Yemen. Source: http://www.usatoday.com/news/nation/2010-11-01-1Acargo01_CV_N.htm?csp=34news

Water and Dams

Americans value water more than energy, and want government to fix leaking pipes. America's drinking water and wastewater infrastructure is aging at the cost of wasted water and the risk of contamination, according to advocates for increased public funding for repairs. Ninety-five percent of Americans said water delivery is more important than access to energy sources and Internet and cell phone service, according to a survey released the week of October 25 by ITT. ITT also asked survey participants if they thought federal, state, and local governments should invest more in repairing aging pipes and treatment facilities. The answer any water engineering company wants to hear: Yes, by 85 percent. TT reached out to 1,605 people representative of 2006 voting population demographics over the phone, asking 82 questions. The opinions are important, experts said, given that some pipes that carry water are more than 100 years old. The survey indicated Americans are willing to take some of the cost of repairs on themselves, paying on average $6.20, or 11 percent, more per month for water service. ITT estimated that if 63 percent of Americans paid $6.20 more

each month, the nation could collect at least $5 billion per year to fix water infrastructure and secure long-term access to clean water. Source: http://blogs.nationalgeographic.com/blogs/news/chiefeditor/2010/11/american-water-infrastructure-expensive-fixes.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**